Paper ID: MISS21_29

Reinforcement of the Multi-Cloud Infrastructure with Edge Computing

L. Steffina Morin*, P. Murali

SRM Institute of Science and Technology, Tamil Nadu, India

*Corresponding author

Abstract

Background: Cloud computing and the Edge computing are two new technologies that have the potential to improve people's daily lives [1]. Furthermore, the integration of Cloud computing and Edge computing has been enhancing the productivity of a vast range of applications in industries such as supply chains, commercial, engineering, and manufacturing, among others.

Objectives: Security is currently a major concern in Cloud-Edge computing. Modern Edge Cloud security is based on a collection of naive security services such as distribution of keys, authentication, and access control, which are typically deployed at the Cloud as well as Edge level. In recent years, a number of privacy-preserving models and security techniques have been created by a wide range of academics for this goal [2]. Despite this, they have failed to meet the most recent Cloud-Edge user's security expectations.

Methodology: Cloud-Edge infrastructure comprises of user accounts, servers, storage systems, and networks [3]. Protection of sensitive data in the Cloud-Edge environment which can be collected over the Edge devices can be done by authentication, access control, secure data storage, key provisioning, data loss prevention (DLP), and in terms of user revocation.

Results and Discussion: Security is not limited to the Cloud but also with end user device security. We should be aware of the endpoint devices used by administrators to connect with the database. These edge devices should be secured, and connections from unknown or untrusted devices should be denied. Sessions should be monitored to detect suspicious activity. In this paper, we have proposed the private Cloud-Edge infrastructure using Openstack with features of user authentication, access control, secure communication, data loss prevention (DLP), monitoring the users accounts and data storage and in-transit, least privilege and in terms of user revocation [4].

Conclusions and Future Work: Hence, the process of limiting potential weaknesses makes the Cloud-Edge infrastructure with Openstack vulnerable to cyber-attacks. Complex security needs at the cloud's edge entail the provision of a large number of basic services [5]. Future work in this area can be done by introducing new light weight cryptographic schemes with the infrastructure to reduce the computational complexity of cloud and edge-based applications.

References

[1] Wang L, Yang Z, Song X (2020) SHAMC: A Secure and highly available database system in multi-cloud environment. Future Gener Comput Syst 105:873-83.

[2] Chadwick DW, Fan W, Costantino G, De Lemos R, Di Cerbo F, Herwono I, Manea M, Mori P, Sajjad A, Wang XS (2020) A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Gener Comput Syst 102:710-722

[3] Wang T, Mei Y, Jia W, Zheng X, Wang G, Xie M (2020) Edge-based differential privacy computing for sensor–cloud systems. J Parallel Distrib Comput 136:75-85.

[4] Couto RS, Sadok H, Cruz P, da Silva FF, Sciammarella T, Campista ME, Costa LH, Velloso PB, Rubinstein MG (2018) Building an IaaS cloud with droplets: a collaborative experience with OpenStack. J Netw Comput Appl 117:59-71.

[5] Thabit F, Alhomdy S, Al-Ahdal AH, Jagtap S (2021) A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Glob Transit Proc 2(1):91-99.

Published by AIJR Publisher in "Abstracts of 1st International Conference on Machine Intelligence and System Sciences (MISS-2021), 1–2 November 2021. Organized by the Techno College of Engineering Agartala, Tripura, INDIA. DOI: 10.21467/abstracts.120

ISBN: 978-81-954993-2-8